REMARKS

Claims 1-24 are pending in this Application. The Office Action dated August 22, 2006, finally rejected all of the currently pending claims. In the present response, no claims have been amended, no claims have been canceled, and no claims are added. Thus, with the entry of the present response, Claims 1-24 remain pending. For at least the reasons discussed in detail below, each of the presently pending claims is in condition for allowance.

Claim Rejections - 35 U.S.C. § 102

Claims 1-24 are rejected under 35 U.S.C. 102(e) as being anticipated by Bowman et al, U.S. Patent No. 6,751,736. Applicant respectfully traverses the rejections.

For example, Applicant respectfully submits that Bowman does not anticipate nor render obvious at least the limitation of claim 1 of enabling at least the encrypted string to be locally decrypted at the user node. After a careful review of Bowman, and in particular, the locations within Bowman identified by the Office Action, the Applicant was unable to identify anywhere Bowman teaches or even suggests at least this limitation.

The Office Action points to Column 5 lines 41-48 stating that Bowman discloses a **local** CGI script that calls and uses the necessary decoding and decrypting algorithms. The Applicant respectfully disagrees. Instead, Bowman merely discloses "the displayable string containing the encoded and encrypted product information is appended to a URL value..., which points to a Common Gateway Interface (CGI) script which executes and/or calls the decoding and decrypting algorithm...." However, it was commonly recognized at the time the invention was made that such network called CGI scripts did not execute on the local client's computer, but rather were executed remotely on the web server. As shown in Bowman, and in particular in FIGS 1-3, the CGI script is accessed (and executes remotely) at "http://www.example.com/cgi-bin." Thus, Bowman does not disclose or suggest enabling the encrypted string to be **locally** decrypted, for at least the reason that the CGI script does not execute locally on the user's computer.

Equally relevant, a careful review of Bowman discloses that the encrypted string appears not to be decrypted at the user's computer at all! Rather, the secret string is known by the ultimate recipient of the VBC, e.g., the addressee designated in the CGI URL to which the VBC is sent after the user actuates the GUI device to transmit his buy order or other WWW message. See Bowman, Col. 7, lines 19-24. The specified destination (URL) is preferably a cash register server computer, which is loaded with software capable of decoding and decrypting the encrypted and encoded data, e.g., the VBC. See Bowman, Col 13, lines 11-17. Thus, it appears that nowhere does Bowman disclose or suggest that the user's computer decrypts or decodes the encrypted string. Such decrypting and decoding of the encrypted string is therefore disclosed as being performed somewhere other than at the user's computer. Therefore, for at least these reasons, Bowman neither anticipates nor renders obvious at least claim 1.

Claim 1 further recites, concatenating data from a plurality of fields of a requested web page into a string. After a careful review of Bowman, the Applicant is unable to identify anywhere that discloses such limitation. Bowman merely discloses that the virtual bar code (VBC) data may include product descriptive information that may be, for example, imported from a database, collected by a CGI script which processes another web page form into which the merchant enters the data, or collected via a special program which embodies the algorithm. See Bowman, Col. 7, 1-12. Bowman, however, does not disclose that the data is from a plurality of fields of a requested web page, as claimed. A quick look at the Applicant's FIG. 2a makes clear that the data that the Applicant refers to in at least claim 1, is not the same product descriptive information disclosed by Bowman.

Moreover, Bowman's user data collected using CGI scripts does not disclose or suggest concatenating data from a plurality of fields of a requested web page into a string that is then encrypted. While Bowman's user submitted data, which may be obtained through the use of form sections such as described in Bowman at Col. 5, lines 41-Col 6, line 65, does appear to be concatenated with the encrypted string (see, e.g., Bowman, Col 6, lines 5-11; Col 6, and lines 49-55); however, such user data does not appear to be part of the string that is then encrypted. **This distinction is important.** Bowman maintains the user data unencrypted from (distinct from) the

other encrypted encoded data. As disclosed by Bowman later, the received data is parsed to separate the user input data 1055, from the encrypted encoded data 1060. See Bowman, Col 11, lines 52-53. In another embodiment, Bowman discloses that the encoded encrypted data will be communicated per HTTP in separate variables than the user input data, so they will not need to be separated by parsing. See Bowman, Col. 11, lines 58-60. Thus, it is clear that Bowman does not disclose concatenating data from a plurality of fields of a requested web page into a string. And, in particular, Bowman does not disclose or suggest encrypting that string. Thus, for at least this reason, Bowman does not disclose or suggest at least these limitations of claim 1; therefore, claim 1 should be allowed to issue.

Independent claims 16 and 10 include similar, albeit different limitations as recited above for claim 1. For example, claim 16 recites, in part, enabling at least the encrypted string to be locally decrypted at the user node. Claim 16, also recites, in part, concatenating data from a plurality of field of a requested web page into a string, [and] encrypting the string. In addition, claim 10, recites, in part, locally decrypting the encrypted string with [the] security applet. Thus, for at least the same reasons as noted above, Bowman does not anticipate nor render obvious claim 10 and 16, and they too should be allowed to issue.

Claim 10 further recites, in part, distributing a plurality of portions of the decrypted string to the plurality of blank fields in the form. Nowhere, does it appear that Bowman actually suggests or teaches such limitation. Bowman merely discloses a merchant web pages contains an encoded (displayable character), encrypted string containing information about a product that has been provided by a merchant. The encoded encrypted string with other information attached, which is useful in decrypting the string is called a virtual bar code (VBC). See Bowman, Col. 3, line 58-Col. 4, line 1. The displayable character string, random string, and secret ID can be entered separately into the web page code or preferably they can be concatenated together, and included in a section of a web page, which may contain text description, pictures, and other multimedia content pertaining to an item presented for sale. The displayable character string is included in the HTML source code in a manner such that it will be transmitted to a URL target address specified in the web

page. Bowman, Col. 4, line 65 - Col. 5, line 8. This displayable character remains encoded data - and is thus - not decrypted.

Thus, unlike the claimed invention, Bowman does not teach or suggest distributing...the decrypted string to...blank fields in the form, as required at least by claim 10. Thus, for at least these reasons, Bowman cannot anticipate nor render obvious claim 10, and it should therefore be allowed to issue.

Dependent claim 6 recites, in part, receiving login data from the user node encrypted by the security applet that is served to the user node. Nowhere, however, does Bowman even discuss login data, let alone using the security applet served to the user node to encrypt login data. It appears that Bowman's use of the term "secret string" has somehow become confused with login data. See Bowman, Col. 7, lines 18-9, and lines 13-45. Bowman discloses at Col. 7, an algorithm for producing a virtual bar code for inclusion in a web page. In block 421, a secret string used in encrypting the VBC message is input to the algorithm. This secret string, preferably a binary sequence is also known by the ultimate recipient of the VBC. See Bowman, Col. 7, lines 18-24. This secret string however, is not disclosed or even suggested to be login data that is encrypted by the security applet served to the user node. In fact, the process described by FIG 4 appears to be entirely performed at an authoring computer 1103, and not at the shopper's web client computer 1120, as shown in FIG. 11. See Bowman, Col. 11 line 9 - Col. 12, line 45. Thus, for at least these reasons, Bowman does not anticipate nor render obvious at least claim 6. Similarly, because claims 8, 13, 14, 15, 21, 23, and 24, each refer to login data, which is neither disclosed or suggested by Bowman, they are also allowable, and should be permitted to issue.

In addition, Claims 2-9 depend from claim 1; claims 11-15 depend from 10; and claims 17-24 depend from claim 16. Therefore, for at least the same reasons as their respective independent claims, each of the dependent claims is also allowable. Thus, Applicant respectfully submits that Claims 1-24 are in condition for allowance, and should be allowed to issue.

CONCLUSION

By the foregoing explanations, Applicant believes that this response has responded fully to all of the concerns expressed in the Office Action, and believes that it has placed each of the pending claims in condition for immediate allowance. Early favorable action in the form of a Notice of Allowance is urged. Should any further aspects of the application remain unresolved, the Examiner is invited to telephone Applicant's attorney at the number listed below.

Dated: October 23, 2006

Respectfully submitted,
By _____
Jamie L. Wiegand
Registration No.: 52,361
DARBY & DARBY P.C.
P.O. Box 5257
New York, New York 10150-5257
(206) 262-8915 ▫ (212) 527-7701 fax
Attorneys/Agents For Applicant